D. ASHELY, BELL, and JONES Do Not Have Federal Firearms Licenses

15. Based on my involvement in this investigation, as well as conversations with other law enforcement agents involved in the investigation, I am aware of the following:

a. As of May 22, 2017, and based on a query of the ATF's National Licensing Center's Federal Licensing System by ATF Special Agent Larry Wozniak, ASHLEY, BELL, and JONES do not have Federal Firearms Licenses.

b. On May 11, 2017, Special Agent Wozniak queried the National Firearms Registration and Transfer Record for results pertaining to ASHELY, BELL, and JONES. The results of this query show that ASHLEY, BELL, and JONES have no approved applications for the transfer of any weapons that require NFA approval (i.e. fully automatic firearms).

E. Additional Investigation of the SUBJECT VEHICLE and SUBJECT PREMISES

16. Based on my personal involvement in this investigation and discussions with other agents, I am aware of the following:

a. On August 31, 2016, during a traffic stop of the SUBJECT VEHICLE, ASHLEY was found in possession of a semi-automatic Sig Sauer .40 caliber hand gun.

b. On November 21, 2016, ASHLEY pled nolo contendere to a violation of California Penal Code section 25850(a), carrying a loaded firearm in public.

17. Based on my personal involvement in this investigation and discussions with other agents, I am aware of the following:

a. On October 6, 2016, the Hon. Steven Kim, United States Magistrate Judge, authorized the installation of a GPS tracking device on the SUBJECT VEHICLE. On October 11, 2016, a GPS tracking device was installed on the SUBJECT VEHICLE while parked in front of the SUBJECT PREMISES.

b. During the monitoring period from October 11, 2016, to November 25, 2016, the GPS tracking device showed the SUBJECT VEHICLE parked at the SUBJECT PREMISES on a majority of the nights.[6]

c. At the time the GPS tracking device was removed from the SUBJECT VEHICLE, it was parked in front of the SUBJECT PREMISES.

18. Based on my personal involvement in this investigation and discussions with other agents, I am aware of the following:

a. On March 8, 2016, law enforcement conducted surveillance of the SUBJECT PREMISES, during which the SUBJECT VEHICLE was seen parked in front of the SUBJECT PREMISES. Law enforcement also observed ASHLEY and an unidentified male exit the SUBJECT PREMISES and enter a Chevrolet Camaro parked in the driveway of the SUBJECT PREMISES.

19. Based on my review of public records, I am aware that the SUBJECT PREMISES is owned by "Ed Dixie." Based on law enforcement investigation and surveillance, there is no

[6] The SUBJECT VEHICLE is registered to ASHLEY at the SUBJECT PREMISES.

indication that an individual known as "Ed Dixie" currently lives at the SUBJECT PREMISES. Rather, public records indicate that since 1998, ASHLEY has listed the SUBJECT PREMISES as his residence.

20. Based on my review of California Department of Motor Vehicles ("DMV") records, I am aware of the following:

a. ASHLEY's current California driver's license lists his address as the SUBJECT PREMISES, with an application date of September 8, 2011.

b. A review of DMV databases for vehicle registration records associated with ASHLEY indicates that the SUBJECT VEHICLE is registered to ASHLEY at the SUBJECT PREMISES.

F. Training and Experience Regarding Firearms and Narcotics Traffickers Use of Home and Car

21. Based on my training and experience, as well as the training and experience of other investigators in this case with whom I have consulted, I am familiar with the *modus operandi* of persons involved in the illegal distribution of narcotics and firearms. Based on this, I familiar with the following:

a. Persons involved in illicit distribution of narcotics or firearms routinely attempt to conceal their identities as well as the location at which drug/gun transactions take place. These people are also known to have vehicles, properties, telephones, utilities, and other items purchased in the names of others, and through the use of stolen

identities, in order to conceal the association of drug/gun activities with their true identity and financial transactions.

b. Individuals engaged in organized narcotics and firearms distribution and sales maintain extensive contact with persons from whom they receive drugs/guns and with whom they distribute these drugs/guns, and in doing so, often utilize coded language to disguise their activity.

c. Narcotics and firearm traffickers maintain on hand large amounts of U.S. currency, as proceeds of their gun and drug sales, in order to maintain and finance their ongoing narcotics activities and other businesses, as well as paying for vehicles, clothing, jewelry, firearms, entertainment, living expenses, bills, acquiring assets, and making other purchases.

d. Persons engaged in narcotics and firearms trafficking conceal in their vehicles and residences, the residences of their associates, residences of family members, and associated businesses or other locations where the offenders may hang-out, proceeds of their drug and gun transactions to include, records of drug/gun transactions, large amounts of currency, money counters, financial instruments, precious metals and gems, jewelry, stolen or counterfeit goods, and other items of value.

e. Persons engaged in narcotics trafficking conceal in their vehicles and residences, the residences of their associates, residences of family members, and associated businesses or other locations where the offenders may hang-out,

various amounts and types of narcotics, scales, vials, blenders, baggies, bindles, balloons, foil, plastic wrap, cutting agents and adulterants, cutting boards, cutting and mixing tools, and other items used in preparing, manufacturing, packaging, distributing, transporting, and selling narcotics, as well as items such as pipes, tubes, syringes, spoons and items used to mix, administer, ingest, inhale, or otherwise use the narcotics.

f. Persons engaged in narcotics and firearms trafficking conceal in their vehicles and residences, the residences of their associates, residences of family members, and associated businesses or other locations where the offenders may hang-out, firearms, magazines, ammunition, weapons cases/bags, knives, and other weapons and weapon accessories. Additionally, these offenders commonly keep these items in nearby bushes, planter boxes, trash cans, barbeque grills, bumpers and tire wells of vehicles, and other similar locations outside of the residences and business, in easy-to-reach locations in and around their area of operation.

g. Most firearms kept and/or made accessible to gang members and drug/gun traffickers are not registered to the offender and the firearm may be modified. Furthermore, it is common for drug/gun traffickers to carry and or use firearms in furtherance of drug/gun transactions and other violent crimes.

h. Individuals involved in firearms and narcotics trafficking often maintain records linking them to their trafficking and that these records may include records of

firearms and/or narcotics customers and associates, sales, debts, and shipments. The records/documents may include receipts of wire transfer transactions, banking/ATM receipts, shipping receipts from postal and shipping businesses, telephone records, telephone books which identify customers and/or co-conspirators, and photographs of co-conspirators. Even if off-site locations are used to store the above records, some evidence such as safety deposit keys, records, and receipts and/or documents regarding multi-warehouses, storage facilities, mail and answering services may be present.

i. Individuals involved in firearms and narcotics trafficking heavily utilize cellular telephones and other electronic devices to communicate with one another and that these devices often contain indicia of the identity of individual and his/her associates, as well as their criminal activity, including but not limited to, call logs, voicemail messages, text messages, electronic messages (e-mail), photographs, videos, address books, calendars, notes, and ledgers.

j. Individuals involved in narcotics and firearms trafficking often utilize social networking websites on the internet, which are commonly accessed via cellular telephones, to communicate with one another, and post comments, pictures, videos, and music related to their membership and activity in the gang and/or their drug/gun trafficking activity.

G. Training and Experience Regarding Digital Devices

22. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to

search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before

they are overwritten. In addition, a computer's or digital device's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image

as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be

necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

REQUEST FOR NO KNOCK AND NIGHTTIME SERVICE

23. I request that the Court authorize investigators to serve this warrant during the nighttime, as set forth under Fed. R. Crim. Proc. 41(e)(2)(A)(ii). Good cause exists because the SUBJECT PREMISES is associated with an individual who is suspected of firearms possession and trafficking. Given the holding set forth in *Gooding v. United States*, 416 U.S. 430 (1974), that there is no need for the presence of exigent circumstances in narcotics cases to justify a nighttime search, I believe that nighttime service is warranted in this case. In addition, nighttime service is justified in this case given the nature of the location being entered. Law enforcement believes firearms are located at the SUBJECT PREMISES and/or the SUBJECT VEHICLE, both of which are located inside a fenced-in area. If law enforcement were to execute this warrant during the day

time, it would be very hard for law enforcement to evade detection and would, thus, pose a risk for officer safety.

24. For the same reasons, including the safety concerns based on ASHLEY's suspected weapons possession, I am requesting authorization for a "no-knock entry" of the SUBJECT PREMISES. Based on the evidence described above, I believe knocking and announcing entry would be dangerous to the agents serving the warrant and would also allow the destruction of evidence.

CONCLUSION

25. For all the reasons described above, there is probable cause to believe that evidence of violations of the SUBJECT OFFENSES, as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachment A of this affidavit.

/s/

Christopher Rumph,
Special Agent, Drug
Enforcement Administration

Subscribed to and sworn before me
this 5th day of ~~May~~ June, 2017.

STEVE KIM

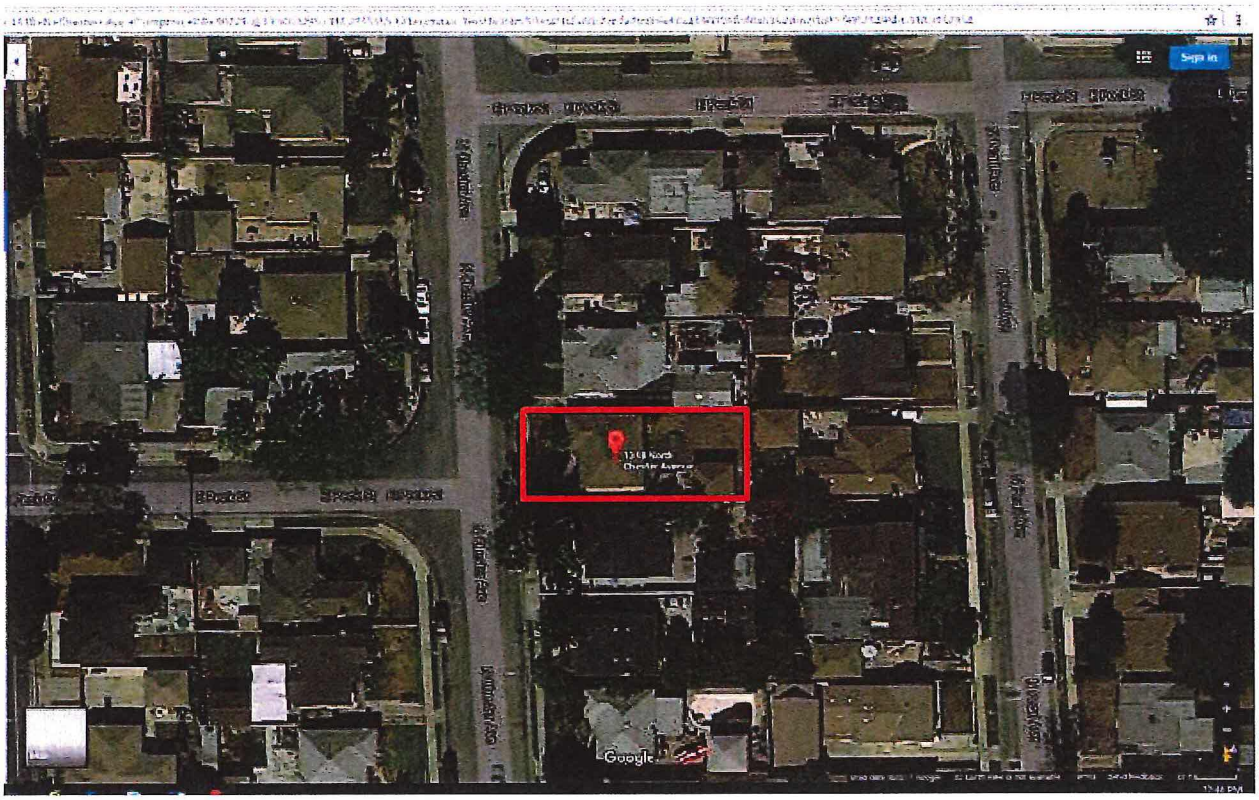
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The premises is located at 1318 North Chester Avenue, Compton, California, 90221 (the "SUBJECT PREMISES"), including all garages and storage areas which are assigned to SUBJECT PREMISES, whether attached to or detached from SUBJECT PREMISES. The SUBJECT PREMISES is further described as a pale pink residence with a front yard separated from the sidewalk by a metal gate, a driveway running alongside the main structure, and a backyard which contains an outbuilding. The SUBJECT PREMISES is further depicted in the photographs below.

ATTACHMENT A-1



ATTACHMENT A-2

PROPERTY TO BE SEARCHED

The property to be searched is a gold 2007 Buick Lucerne bearing Vehicle Identification Number 1G4HD57267U152262, California license plate number 7UCU803, and registered to "Marquis C. Ashley," at 1318 Chester Ave., Compton, California, 90221.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized from the SUBJECT PREMISES are the fruits, instrumentalities, and evidence of violations of the following offenses 18 U.S.C. § 371, dealing firearm without a license, in violation of 18 U.S.C. § 922(a), possession of unregistered firearms, in violation of 26 U.S.C. § 5861(d), and conspiracy to distribute narcotics, in violation of 21 U.S.C. § 846 (collectively, the "Subject Offenses"), namely:

a. Any controlled substance, including phencyclidine;

b. Materials and equipment used to package controlled substances, including but not limited to, plastic wrap, shrink wrap materials, tape, odor-disguising substances, and scales;

c. Materials and equipment used to package or transport currency including, but not limited to, plastic wrap, shrink wrap materials, money-counting machines, money wrappers, rubber bands, duct tape or wrapping tape, and plastic sealing machines;

d. Any documents or materials reflecting or relating to the shipment of packages through Federal Express, the United States Postal Service, or other common carriers, including, but not limited to, packaging supplies, packing slips, tracking numbers, and receipts.

e. Any records, documents, programs, applications, or materials showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, including but not limited to, documents written in vague or coded language, bank account records, wire transfer records, bank statements, pay-owe sheets, receipts, safe deposit box keys and records, money containers, financial records, and related documents;

f. Any drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

g. Any United States currency over $1,000 or bearer instruments worth over $1,000 (including cashier's checks and traveler's checks);

h. Any records, documents, programs, applications, or materials reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other items commonly obtained with the proceeds of drug trafficking activities;

i. Items of personal property reflecting names, addresses, telephone numbers, or communications of members or associates involved in drug trafficking activities, including, but not limited to, personal telephone books, address books, telephone bills, photographs, videotapes, facsimiles, personal

notes, cables, telegrams, receipts, and documents and other items;

j. Any weapons, including but not limited to: knives, firearms (including pistols, handguns, shotguns, rifles, assault weapons, and machine guns), firearm magazines, firearm components (including components or tools which can be used to modify firearms or ammunition), firearm accessories, ammunition, and tools used for the manufacture of ammunition (including reloading devices, dies, scales, books, pamphlets, and documentation);

k. Any documentation, records, receipts, luggage tags, boarding passes, or the like, relating to the movement, transportation, or shipment of firearms;

l. Any documentation, records, receipts, certification, licenses, or the like, relating to the sale, transfer, purchase, or movement of firearms;

m. Any bills and/or subscriber documents related to digital devices used to facilitate the Subject Offenses;

n. Any indicia of occupancy, residency, or ownership of the premises to be searched and things described in the warrant, including, but not limited to: forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing; and

o. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

p. With respect to any digital device used to facilitate the above-listed Subject Offenses or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. Evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. Evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. Evidence of the attachment of other devices;

iv. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. Evidence of the times the device was used;

vi. Passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. Records of or information about Internet Protocol addresses used by the device; and

ix. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical

disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to

determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.